



---

## Analisis Yuridis Pertanggungjawaban Pidana Penyelenggara Sistem Elektronik Artificial Intelligence Atas Manipulasi Data Biometrik Orang Lain Dalam Penipuan Transaksi Elektronik

Desak Kadek Era Dewi Susanti<sup>1</sup>, Ni Putu Rai Yuliantini<sup>2</sup>, Dewa Gede Sudika Mangku<sup>3</sup>.

Fakultas Hukum dan Ilmu Sosial, Universitas Pendidikan Ganesha, Indonesia,<sup>1-3</sup>

Email Korespondensi: [desak.era@student.undiksha.ac.id](mailto:desak.era@student.undiksha.ac.id)<sup>1</sup>, [raiyluliantini@undiksha.ac.id](mailto:raiyluliantini@undiksha.ac.id)<sup>2</sup>, [sudika.mangku@undiksha.ac.id](mailto:sudika.mangku@undiksha.ac.id)<sup>3</sup>

---

Article received: 01 Januari 2026, Review process: 12 Januari 2026

Article Accepted: 22 Maret 2026, Article published: 01 Mei 2026

---

### ABSTRACT

*This study aims to analyze the regulation and criminal liability of Artificial Intelligence Electronic System Providers (PSE) for biometric data manipulation in electronic transaction fraud. This study uses a normative juridical method with a statutory and conceptual approach, as well as secondary data analyzed descriptively qualitatively. The results of the study indicate that legal regulations related to biometric data manipulation are still scattered in several regulations, such as the ITE Law, the PDP Law, and the Criminal Code, and there is no *lex specialis* that specifically regulates Artificial Intelligence. PSE criminal liability can be based on the doctrine of fault, both intentional and negligent. However, law enforcement still faces obstacles due to the lack of specific binding regulations, so the formation of stricter regulations is needed to ensure legal certainty.*

**Keywords:** Criminal Liability, Electronic System Organizers, Artificial Intelligence, Biometric Data Manipulation.

### ABSTRAK

Penelitian ini bertujuan untuk menganalisis pengaturan dan pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) *Artificial Intelligence* atas manipulasi data biometrik dalam penipuan transaksi elektronik. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual, serta data sekunder yang dianalisis secara deskriptif kualitatif. Hasil penelitian menunjukkan bahwa pengaturan hukum terkait manipulasi data biometrik masih tersebar dalam beberapa regulasi, seperti UU ITE, UU PDP, dan KUHP, serta belum adanya *lex specialis* yang secara khusus mengatur *Artificial Intelligence*. Pertanggungjawaban pidana PSE dapat didasarkan pada doktrin kesalahan, baik kesengajaan maupun kelalaian. Namun, penegakan hukum masih menghadapi kendala akibat belum adanya pengaturan khusus yang mengikat, sehingga diperlukan pembentukan regulasi yang lebih tegas untuk menjamin kepastian hukum.

**Kata Kunci:** Pertanggungjawaban Pidana, Penyelenggara Sistem Elektronik, Artificial Intelligence, Manipulasi Data Biometrik.

## PENDAHULUAN

Perkembangan Perkembangan teknologi informasi digital berbasis internet sebagai sumber informasi mengalami peningkatan yang sangat pesat (Yudiawan dkk, 2023:70). Hal tersebut turut mendorong terjadinya perubahan besar dalam dunia digital yang memiliki peran penting dalam proses penyebaran informasi kepada masyarakat (Aprianto, 2021:8). Teknologi digital yang diimplementasikan dengan baik dapat menjadi sarana yang efektif dalam memberdayakan masyarakat, meningkatkan keterampilan, serta mendukung berbagai aktivitas ekonomi dan sosial (Trisiana dkk., 2025:47). Teknologi digital tidak hanya berfungsi sebagai alat komunikasi, tetapi juga telah berkembang menjadi infrastruktur yang mendukung berbagai aktivitas sosial, ekonomi, pendidikan, maupun pemerintahan (Hartono dkk, 2020:283). Kondisi ini menunjukkan bahwa teknologi digital telah menjadi bagian penting dalam kehidupan masyarakat modern karena mampu memberikan kemudahan, efisiensi, serta kecepatan dalam menjalankan berbagai aktivitas yang sebelumnya dilakukan secara konvensional. Apalagi dalam hal hiburan, rutinitas dan aktivitas sehari-hari seringkali menimbulkan kejenuhan yang dapat menyebabkan stres. Oleh karena itu, menikmati hiburan menjadi hal yang penting dalam menjaga keseimbangan aktivitas sehari-hari, yang kini juga semakin mudah diakses melalui pemanfaatan teknologi digital (Yuliantini dkk, 2022:475). Seiring dengan meningkatnya pemanfaatan teknologi digital, persaingan di era digital juga semakin ketat sehingga menuntut perusahaan untuk terus melakukan inovasi serta menyesuaikan strategi bisnis agar tetap relevan dan mampu bersaing dalam industri (Syaifudin dkk., 2025:1081).

Pembangunan suatu negara terwujud melalui peran dan tanggung jawab pemerintah semata serta dukungan dari seluruh komponen masyarakat, terutama pelaku usaha, untuk menciptakan kesejahteraan sosial dan meningkatkan kualitas hidup masyarakat (Windari dkk, 2024:8). Perkembangan teknologi digital dalam bidang ekonomi turut mendorong terjadinya transformasi di berbagai sektor industri. Pelaku usaha semakin memanfaatkan teknologi digital dalam menjalankan kegiatan bisnis, khususnya dalam pemasaran, pengelolaan data, serta pelaksanaan transaksi. Sistem transaksi elektronik terus berkembang pesat karena memberikan kemudahan bagi masyarakat dalam melakukan aktivitas ekonomi secara lebih cepat, praktis, dan efisien tanpa dibatasi oleh ruang dan waktu.

Pesatnya perkembangan teknologi tersebut juga mendorong munculnya berbagai inovasi teknologi baru yang semakin canggih. Salah satu inovasi teknologi yang berkembang pesat dalam beberapa tahun terakhir adalah *Artificial Intelligence* (AI). Kecerdasan Buatan *Artificial Intelligence* (AI) adalah kemampuan yang diterapkan pada sebuah sistem yang dapat diatur dalam kerangka ilmiah (Sukmaningsih, 2025:17). *Artificial Intelligence* (AI) pada dasarnya merupakan kemampuan yang dimiliki oleh sistem komputer atau mesin untuk meniru proses kognitif manusia, seperti belajar, berpikir, menalar, serta memecahkan permasalahan. Teknologi ini dikembangkan dengan tujuan untuk menciptakan sistem yang mampu bekerja secara cerdas dan mandiri, termasuk dalam mengambil keputusan serta menyesuaikan diri terhadap kondisi atau situasi baru tanpa harus diprogram secara khusus untuk setiap kemungkinan yang terjadi (Rojabi, 2025:7).

Dalam penerapannya, perkembangan teknologi digital juga diikuti dengan penggunaan sistem verifikasi identitas berbasis data biometrik dalam berbagai layanan elektronik. Biometrik berasal dari kata "*bios*" yang berarti kehidupan dan "*metric*" yang berarti ukuran atau pengukuran. Secara sederhana, biometrik dapat dipahami sebagai metode untuk melakukan pengukuran serta analisis terhadap karakteristik biologis maupun perilaku yang dimiliki oleh setiap individu (Ermeitha, 2025:8). Dalam Penjelasan Pasal 4 Ayat (2) Huruf b Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mendefinisikan data biometrik sebagai berikut: "*Yang dimaksud dengan "data biometric adalah data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap individu, seperti gambar wajah atau data daktiloskopi. Data biometrik juga menjelaskan pada sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, termasuk namun tidak terbatas pada rekam sidik jari, retina mata, dan sampel DNA.*"

Sehingga data biometrik dapat berupa berbagai karakteristik fisik maupun biologis yang melekat pada diri seseorang dan dapat digunakan untuk mengidentifikasi identitas individu secara unik. Bentuk data biometrik tersebut antara lain wajah (*face recognition*) yang digunakan dalam sistem pengenalan wajah, sidik jari (*fingerprint*) yang banyak dimanfaatkan pada perangkat *smartphone* maupun sistem keamanan digital, retina atau iris mata yang digunakan dalam sistem identifikasi dengan tingkat keamanan yang tinggi, suara (*voice recognition*) yang digunakan dalam proses verifikasi identitas melalui pengenalan suara, serta DNA yang digunakan dalam proses identifikasi biologis seseorang.

Karakteristik-karakteristik tersebut memiliki sifat yang unik pada setiap individu sehingga sering digunakan sebagai metode autentikasi dalam berbagai sistem elektronik untuk memastikan keaslian identitas pengguna. Penggunaan teknologi biometrik dalam sistem elektronik bertujuan untuk meningkatkan keamanan serta memastikan keaslian identitas pengguna dalam mengakses layanan digital. Oleh karena itu, banyak penyelenggara sistem elektronik yang memanfaatkan teknologi biometrik sebagai metode autentikasi dalam berbagai layanan, termasuk dalam sistem transaksi elektronik. Namun demikian, pesatnya perkembangan teknologi juga membuka peluang terjadinya berbagai bentuk penyalahgunaan teknologi oleh pihak-pihak yang tidak bertanggung jawab. Dengan memanfaatkan teknologi tertentu, identitas biometrik seseorang dapat dimodifikasi atau ditiru sehingga tampak seolah-olah asli. Kondisi ini dapat dimanfaatkan oleh pelaku kejahatan untuk melakukan berbagai tindakan yang merugikan pihak lain, termasuk melakukan penipuan dalam transaksi elektronik dengan menggunakan identitas orang lain yang telah dimanipulasi secara digital.

Teknologi *Artificial Intelligence* (AI) memungkinkan sistem komputer untuk mengolah, menganalisis, dan merekayasa berbagai jenis data secara otomatis dengan tingkat akurasi yang tinggi. Teknologi ini tidak hanya dimanfaatkan untuk analisis data dan otomatisasi pekerjaan, tetapi juga mampu memproses data visual dan audio secara lebih kompleks, sehingga dapat menghasilkan simulasi digital yang menyerupai kondisi nyata, termasuk mereplikasi wajah, suara, maupun ekspresi seseorang. Namun demikian, di sisi lain teknologi *Artificial Intelligence* juga

berpotensi disalahgunakan untuk tujuan yang melanggar hukum, salah satunya melalui manipulasi data biometrik seperti wajah dan suara sehingga tampak seolah-olah berasal dari individu yang sebenarnya. Penyalahgunaan ini dapat menimbulkan kerugian, terutama apabila digunakan dalam transaksi elektronik, karena pelaku kejahatan dapat menyamar sebagai orang lain untuk mengakses sistem yang menggunakan autentikasi biometrik dan melakukan transaksi secara tidak sah, yang pada akhirnya merugikan individu yang identitas biometriknya digunakan tanpa izin.

Peran Penyelenggara Sistem Elektronik (PSE) atau perusahaan penyedia teknologi *Artificial Intelligence* (AI) menjadi sangat penting dalam perkembangan teknologi digital saat ini. Sebagai pihak yang mengembangkan, mengelola, dan mengoperasikan sistem *Artificial Intelligence* (AI), penyelenggara sistem elektronik pada dasarnya memiliki kendali terhadap teknologi yang mereka ciptakan. Namun dalam praktiknya, banyak perusahaan teknologi yang terus berlomba menghadirkan berbagai fitur berbasis kecerdasan buatan yang semakin canggih, seperti teknologi pengubah wajah maupun peniru suara, tanpa diimbangi dengan sistem keamanan yang memadai untuk mencegah potensi penyalahgunaan teknologi tersebut. Padahal kemampuan *Artificial Intelligence* (AI) dalam merekayasa data visual dan audio dapat menghasilkan representasi digital yang menyerupai identitas asli seseorang, sehingga berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk melakukan berbagai bentuk kejahatan, termasuk penipuan dalam transaksi elektronik.

Kondisi tersebut menimbulkan pertanyaan mengenai sejauh mana tanggung jawab penyelenggara sistem elektronik terhadap penyalahgunaan teknologi yang mereka kembangkan. Meskipun perusahaan teknologi sering berpendapat bahwa mereka hanya menyediakan sarana teknologi, dalam perspektif hukum penyelenggara sistem elektronik tetap memiliki kewajiban untuk memastikan sistem yang mereka kelola bersifat andal, aman, dan bertanggung jawab sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik. Sehingga, apabila teknologi yang dikembangkan justru membuka peluang terjadinya manipulasi data biometrik dalam penipuan transaksi elektronik, maka perlu dilakukan kajian hukum lebih lanjut mengenai batas dan bentuk pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) guna memberikan kepastian hukum serta perlindungan bagi masyarakat.

Hukum sebagai pranata sosial memiliki peranan penting dalam masyarakat untuk menciptakan ketentraman, keadilan dan keamanan juga mengatur segala perbuatan manusia yang dilarang maupun yang diperintahkan (Kusuma dkk, 2024:2). Teknologi terus berkembang pesat, namun di sisi lain, regulasi yang ada belum secara khusus mengatur terkait *Artificial Intelligence* (AI). Kondisi ini menimbulkan kekosongan norma, terutama terkait batasan tanggung jawab hukum bagi Penyelenggara Sistem Elektronik (PSE) apabila produk yang *Artificial Intelligence* (AI) dikembangkan justru dimanfaatkan sebagai sarana terjadinya

---

kejahatan, seperti manipulasi identitas melalui data biometrik. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengkaji dan menganalisis pengaturan hukum manipulasi data biometrik melalui teknologi *Artificial Intelligence* berdasarkan hukum positif di Indonesia, serta pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) *Artificial Intelligence* atas manipulasi data biometrik orang lain dalam penipuan transaksi elektronik. Oleh karena itu, penulis melakukan penelitian dengan judul **“Analisis Yuridis Pertanggungjawaban Pidana Penyelenggara Sistem Elektronik *Artificial Intelligence* Atas Manipulasi Data Biometrik Orang Lain Dalam Penipuan Transaksi Elektronik”**.

## METODE

Penelitian ini merupakan penelitian hukum normatif yang bertujuan untuk mengkaji Pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) *Artificial Intelligence* atas penyalahgunaan data biometrik orang lain dalam penipuan transaksi elektronik. Penelitian hukum normatif merupakan jenis penelitian yang menitikberatkan pada kajian terhadap hukum tertulis melalui berbagai perspektif. Kajian tersebut mencakup aspek teoritis, historis, serta analisis terhadap struktur dan sistematika peraturan perundang-undangan (Melo dkk., 2025:110). Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menelaah regulasi terkait Sistem Elektronik, Perlindungan Data Pribadi, dan Transaksi Elektronik, sementara pendekatan konseptual digunakan untuk membangun argumen hukum terkait doktrin pertanggungjawaban pidana korporasi dalam pemanfaatan teknologi kecerdasan buatan. Sumber bahan hukum dalam penelitian ini menggunakan data sekunder berupa peraturan perundang-undangan, buku-buku hukum, jurnal ilmiah, dan literatur lain yang berkaitan dengan objek penelitian. Pengumpulan bahan hukum dilakukan melalui studi kepustakaan. Selanjutnya, bahan hukum yang diperoleh dianalisis menggunakan metode analisis deskriptif kualitatif untuk memberikan gambaran yang sistematis mengenai pengaturan dan Pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) berbasis *Artificial Intelligence* atas penyalahgunaan data biometrik orang lain dalam penipuan transaksi elektronik

## HASIL DAN PEMBAHASAN

### *Pengaturan hukum manipulasi data biometrik melalui teknologi *Artificial Intelligence* berdasarkan hukum positif di Indonesia*

Perkembangan teknologi digital yang semakin pesat telah mendorong penggunaan berbagai sistem elektronik dalam aktivitas masyarakat, termasuk dalam pelaksanaan transaksi elektronik. Salah satu teknologi yang banyak digunakan dalam sistem elektronik adalah teknologi *Artificial Intelligence* (AI) yang mampu mengolah berbagai jenis data secara otomatis. Dalam praktiknya, teknologi ini juga dapat memproses serta merekayasa data biometrik seperti wajah, suara, sidik jari, maupun karakteristik biologis lainnya. Kemampuan tersebut pada satu sisi

---

memberikan manfaat dalam meningkatkan keamanan sistem elektronik melalui mekanisme autentikasi biometrik, namun di sisi lain juga berpotensi menimbulkan penyalahgunaan, apabila teknologi tersebut digunakan untuk memanipulasi identitas seseorang dalam aktivitas yang melanggar hukum. Salah satunya ialah memanipulasi data biometrik milik orang lain.

Manipulasi merupakan suatu tindakan rekayasa yang dilakukan secara sengaja dengan cara menambah, menyembunyikan, menghilangkan, atau mengaburkan sebagian maupun seluruh informasi, substansi, realitas, fakta, data, ataupun catatan sejarah. Tindakan tersebut dilakukan melalui suatu proses yang dirancang secara sistematis dan dapat dilakukan oleh individu, kelompok, maupun dalam suatu sistem tertentu (Ablisar dkk., 2022:54). Dalam hal teknologi digital, manipulasi dapat terjadi terhadap berbagai jenis data yang tersimpan dalam sistem elektronik, termasuk data biometrik. Data biometrik merupakan data yang berkaitan dengan karakteristik fisik, fisiologis, maupun perilaku seseorang yang bersifat unik dan dapat digunakan untuk mengidentifikasi individu secara spesifik. Contoh data biometrik antara lain wajah, sidik jari, retina mata, suara, maupun DNA. Karena memiliki sifat yang unik dan melekat pada individu, data biometrik sering digunakan sebagai metode autentikasi dalam berbagai layanan digital, khususnya dalam sistem transaksi elektronik yang memerlukan verifikasi identitas pengguna.

*Artificial Intelligence (AI)* secara umum dapat dibagi menjadi tiga kategori, yaitu *Artificial Narrow Intelligence (ANI)*, *Artificial General Intelligence (AGI)*, dan *Artificial Superintelligence (ASI)*. *Artificial Narrow Intelligence* merupakan jenis kecerdasan buatan yang dikembangkan untuk menjalankan tugas tertentu secara spesifik sesuai dengan fungsi yang telah diprogramkan, seperti teknologi asisten suara atau sistem pengenalan wajah. Sementara itu, *Artificial General Intelligence* merupakan konsep kecerdasan buatan yang dirancang untuk meniru kemampuan intelektual manusia secara menyeluruh sehingga mampu berpikir, belajar, serta menyelesaikan berbagai tugas secara mandiri tanpa bergantung pada arahan manusia (Haris dkk, 2022:308). Dari ketiga jenis tersebut, *Artificial Narrow Intelligence (ANI)* merupakan jenis *Artificial Intelligence* yang paling banyak digunakan dalam praktik saat ini, karena dirancang untuk menjalankan tugas tertentu secara spesifik, seperti pengenalan wajah, pengenalan suara, maupun analisis gambar. Teknologi ini umumnya didukung oleh metode *machine learning*, *deep learning*, serta *computer vision* yang memungkinkan sistem komputer mempelajari pola data visual maupun audio secara otomatis (Heidari dkk, 2024:4). Beberapa contoh aplikasi berbasis *Artificial Narrow Intelligence (ANI)* yang memiliki kemampuan untuk memanipulasi data biometrik secara spesifik meliputi platform rekayasa visual seperti *DeepFaceLab*, *Reface*, dan *MyHeritage* yang mampu menghasilkan *deepfake* wajah dengan presisi tinggi. Untuk manipulasi audio atau *voice cloning*, terdapat aplikasi seperti *ElevenLabs*, *Descript*, dan *VALL-E* yang dapat menduplikasi karakteristik suara seseorang hanya dengan sampel durasi singkat. Selain itu, model kecerdasan buatan generatif multimodal seperti *ChatGPT (OpenAI)* dan *Gemini (Google)* juga memiliki potensi disalahgunakan untuk menciptakan interaksi teks atau suara yang meniru gaya komunikasi spesifik milik orang lain.

Hukum merupakan pilar utama dalam menggerakkan sendi-sendi kehidupan bermasyarakat, berbangsa, dan bernegara (CDM, dkk 2020:49). Dalam menghadapi dinamika lingkungan sosial yang senantiasa berubah, hukum dituntut untuk bersifat adaptif terhadap perkembangan situasi dan kondisi, sehingga tetap mampu menjalankan fungsinya dalam mengatur serta mewujudkan keadilan (Parwati, 2024:14). Indonesia merupakan negara hukum sebagaimana ditegaskan dalam ketentuan Pasal 1 ayat (3) UUD 1945 (Yudiawan dkk, 2021:729). Sehingga menyatakan bahwa setiap tindakan atau perbuatan yang dilakukan oleh individu maupun oleh penyelenggara negara harus berlandaskan pada aturan hukum yang berlaku. Prinsip negara hukum tersebut menegaskan bahwa seluruh kegiatan dalam kehidupan bermasyarakat, termasuk dalam pemanfaatan teknologi digital, wajib tunduk pada ketentuan hukum guna mewujudkan ketertiban, keadilan, serta kepastian hukum. Hal ini sejalan dengan konsep hukum positif sebagai keseluruhan norma atau teks otoritatif yang berlaku dan mengikat dalam kehidupan masyarakat maupun negara (Mangku, 2022:252). Prinsip tersebut juga berlaku dalam penggunaan teknologi *Artificial Intelligence (AI)*, yang dalam pemanfaatannya harus senantiasa berada dalam kerangka pengaturan hukum yang berlaku guna menjamin kepastian dan perlindungan hukum.

Namun demikian, hingga saat ini Indonesia belum memiliki peraturan perundang-undangan yang secara khusus (*lex specialis*) mengatur mengenai teknologi *Artificial Intelligence (AI)* dalam suatu kerangka hukum yang sistematis dan menyeluruh. Ketentuan yang berkaitan dengan pemanfaatan *Artificial Intelligence* masih tersebar dalam berbagai regulasi yang telah ada, sehingga pengaturannya belum berdiri sebagai aturan yang khusus. Oleh karena itu, dalam mengkaji pengaturan hukum manipulasi data biometrik melalui teknologi *Artificial Intelligence* dalam berdasarkan hukum positif di Indonesia, diperlukan penelaahan terhadap beberapa peraturan perundang-undangan yang relevan. Berikut adalah peraturan perundang-undangan terkait manipulasi data biometrik *Artificial Intelligence (AI)* di Indonesia:

a). Kitab Undang-Undang Hukum Pidana

Dalam kerangka hukum positif terbaru Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP Nasional) memberikan penguatan terhadap penindakan manipulasi data biometrik berbasis *Artificial Intelligence*. Melalui Pasal 492 mengenai penipuan dan Pasal 391 mengenai pemalsuan, rekayasa biometrik diposisikan sebagai instrumen tipu muslihat digital yang dilarang.

b). Undang-Undang Informasi Dan Transaksi Elektronik (UU ITE)

Dalam kerangka Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, undang-undang ini telah mengalami beberapa perubahan untuk menyesuaikan dengan perkembangan teknologi informasi. Perubahan pertama dilakukan melalui Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Informasi dan Transaksi Elektronik, kemudian disempurnakan kembali melalui Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik guna menyesuaikan pengaturan hukum dengan perkembangan teknologi digital yang

---

semakin pesat. Teknologi *Artificial Intelligence* diklasifikasikan dilihat dari karakteristiknya, *Artificial Intelligence (AI)* dikategorikan sebagai sistem elektronik sebagaimana dimaksud dalam pasal 1 angka 5 UU ITE. Mengingat *Artificial Intelligence (AI)* beroperasi lewat proses pengumpulan dan pengolahan data. Selain itu, *Artificial Intelligence (AI)* juga bisa dianggap sebagai agen elektronik berdasarkan pasal 1 angka 8 UU ITE, karena mampu bertindak secara otomatis atas instruksi manusia. Terkait dengan manipulasi data biometrik, instrumen hukum utama yang digunakan adalah Pasal 35 UU ITE, yang melarang setiap orang dengan sengaja dan tanpa hak melakukan manipulasi, penciptaan, perubahan, penghilangan, atau pengrusakan informasi elektronik dengan tujuan agar informasi tersebut dianggap seolah-olah data yang autentik. Pelanggaran terhadap ketentuan ini diancam dengan sanksi pidana yang sangat berat sebagaimana diatur dalam Pasal 51 ayat (1), yakni pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). Selain Pasal 35 UU ITE, instrumen hukum dalam UU ITE yang berkaitan erat dengan manipulasi data, regulasi mengenai penyalahgunaan biometrik yang melibatkan teknologi *Artificial Intelligence* juga bertumpu pada Pasal 30 UU ITE terkait akses ilegal, di mana rekayasa biometrik digunakan sebagai sarana untuk menjebol sistem pengamanan (*circumvention*), serta Pasal 32 ayat (1) UU ITE apabila tindakan tersebut menyebabkan pemindahan data pribadi tanpa hak. Secara fundamental, Pasal 15 ayat (1) UU ITE meletakkan beban tanggung jawab kepada Penyelenggara Sistem Elektronik (PSE) untuk menjamin sistem yang andal dan aman. Hal ini mengimplikasikan bahwa jika PSE lalai dalam memitigasi risiko manipulasi *Artificial Intelligence* pada sistemnya sehingga menimbulkan kerugian, maka PSE tersebut dapat dimintai pertanggungjawaban hukum atas kegagalan menyelenggarakan sistem elektronik sebagaimana mestinya.

c). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Pengaturan mengenai manipulasi data biometrik melalui teknologi *Artificial Intelligence* juga dapat ditinjau Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur perlindungan data biometrik melalui Pasal 4 ayat (2) huruf b yang mengklasifikasikan data biometrik sebagai data pribadi yang bersifat spesifik, sehingga pengolahannya, termasuk melalui teknologi *Artificial Intelligence*, memerlukan tingkat perlindungan yang lebih tinggi. Kewajiban tersebut dibebankan kepada Penyelenggara Sistem Elektronik (PSE) sebagai Pengendali Data Pribadi sebagaimana diatur dalam Pasal 35 sampai dengan Pasal 39, yang mewajibkan penyelenggaraan sistem yang aman dari akses tidak sah. Dalam aspek pidana, Pasal 66 melarang pembuatan atau penggunaan data pribadi palsu, termasuk manipulasi identitas melalui, dengan ancaman sanksi dalam Pasal 68 berupa pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp6.000.000.000,00. Selain itu, Pasal 70 memberikan dasar mengenai pertanggungjawaban pidana korporasi, yang memungkinkan Penyelenggara Sistem

---

Elektronik dikenai sanksi apabila sistem yang dikelolanya menyebabkan terjadinya manipulasi data biometrik dalam transaksi elektronik.

- d). Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik

Pengaturan mengenai manipulasi data biometrik melalui teknologi *Artificial Intelligence* juga dapat ditinjau *Artificial Intelligence*. Berdasarkan Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. Dalam Pasal 3 ayat (1), PSE wajib menyelenggarakan sistem elektronik secara andal dan aman, sehingga ketidakmampuan sistem berbasis *Artificial Intelligence* dalam mendeteksi manipulasi biometrik dapat dikualifikasikan sebagai kegagalan pemenuhan standar keandalan sistem. Kewajiban ini dipertegas dalam Pasal 24 ayat (1) yang memerintahkan PSE untuk melindungi data pribadi dari pengolahan yang tidak sah, guna menjaga integritas data biometrik pengguna dari serangan siber. Secara yuridis, Pasal 100 menjadi jembatan hukum yang menetapkan bahwa PSE bertanggung jawab atas segala kerugian yang timbul akibat kegagalan atau kelalaian dalam penyelenggaraan sistem tersebut, baik dalam ranah administratif maupun perdata, terutama jika sistem *Artificial Intelligence* yang digunakan terbukti gagal mencegah terjadinya penipuan transaksi elektronik.

- e). Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial

Perlu dipahami bahwa Surat Edaran (SE) bukan merupakan peraturan perundang-undangan yang memiliki kekuatan hukum mengikat secara umum. Hal ini karena SE tidak termasuk dalam hierarki peraturan perundang-undangan sebagaimana diatur dalam Undang-Undang Nomor 12 Tahun 2011. Oleh karena itu, Surat Edaran lebih bersifat sebagai pedoman atau arahan kebijakan (*soft law*), bukan sebagai aturan hukum yang memberikan sanksi secara langsung. Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial memberikan pedoman bagi Penyelenggara Sistem Elektronik (PSE) dalam menggunakan teknologi berbasis *Artificial Intelligence* (AI). Surat edaran ini menekankan pentingnya prinsip akuntabilitas dan transparansi, di mana PSE bertanggung jawab untuk memastikan bahwa teknologi *Artificial Intelligence* (AI) tidak digunakan untuk menyebarkan informasi yang menyesatkan atau melakukan manipulasi identitas biometrik pengguna. Melalui pedoman tersebut, PSE didorong untuk menerapkan pengelolaan risiko yang baik, termasuk menjaga keamanan data pribadi dan melindungi hak privasi pengguna dari potensi penyalahgunaan teknologi, seperti rekayasa identitas digital dalam transaksi elektronik.

Berdasarkan hasil analisis peraturan perundang-undang tersebut, dapat disimpulkan bahwa meskipun hingga saat ini Indonesia belum memiliki peraturan perundang-undangan yang secara khusus (*lex specialis*) mengatur teknologi *Artificial Intelligence* sebagai subjek hukum yang berdiri sendiri, namun kerangka hukum positif yang berlaku telah membentuk mekanisme perlindungan hukum. Secara normatif, berbagai ketentuan dalam peraturan perundang-undangan yang ada telah memberikan penegasan bahwa setiap tindakan manipulasi data biometrik dengan memanfaatkan teknologi *Artificial Intelligence* merupakan perbuatan yang dilarang oleh hukum dan terhadap pelaku perbuatan tersebut dapat dimintakan

---

pertanggungjawaban hukum sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

### **Pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) *Artificial Intelligence* atas manipulasi data biometrik orang lain dalam penipuan transaksi elektronik**

Hukum pidana sepatutnya mampu memberikan perlindungan terhadap Hak Asasi Manusia, baik bagi pelaku maupun korban tindak pidana, serta menjaga kepentingan masyarakat dan negara secara seimbang dan proporsional (Yuliantini, 2015:81). Dalam hal pertanggungjawaban pidana merupakan proses penjatuhan sanksi kepada pelaku atas perbuatan yang melanggar ketentuan hukum atau menimbulkan keadaan yang dilarang. Sehingga pertanggungjawaban pidana ialah mekanisme pengalihan beban hukuman dari suatu peristiwa tindak pidana kepada individu sebagai pelakunya (Fadlian, 2020:13). Dalam perkembangan teknologi, pesatnya kemajuan *Artificial Intelligence (AI)* tidak hanya memberikan dampak positif, tetapi juga menimbulkan potensi dampak negatif apabila disalahgunakan. Salah satu bentuk penyalahgunaan tersebut adalah penggunaan *Artificial Intelligence (AI)* untuk melakukan manipulasi data biometrik yang kemudian dimanfaatkan dalam tindak pidana penipuan, khususnya dalam transaksi elektronik. Kejahatan ini menjadi semakin rumit karena pelaku dapat memanfaatkan teknologi untuk meniru identitas seseorang secara digital, sehingga sulit dideteksi oleh sistem keamanan konvensional.

Pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) berbasis *Artificial Intelligence* atas manipulasi data biometrik dalam penipuan transaksi elektronik merupakan isu hukum yang rumit, mengingat keterlibatan teknologi sebagai sarana dalam terjadinya tindak pidana. Dalam hukum pidana, suatu pertanggungjawaban hanya dapat dibebankan apabila terpenuhi unsur-unsur tindak pidana, yaitu adanya perbuatan melawan hukum, adanya kesalahan (*mens rea*). Niat (*Mens rea*) merupakan unsur yang sangat penting dalam hukum pidana Indonesia karena berfungsi sebagai dasar dalam menentukan tingkat pertanggungjawaban pidana seseorang. Tanpa adanya unsur niat atau kesengajaan, suatu tindak pidana pada umumnya dianggap belum sempurna, sebab hukum pidana mensyaratkan adanya kesalahan dari sisi batin pelaku yang mendasari perbuatannya (Wirda dkk, 2024:240). Dalam hukum pidana juga harus terdapat unsur perbuatan nyata (*actus reus*), yaitu tindakan konkret yang dilakukan oleh pelaku yang bertentangan dengan hukum Romandona dkk, 2024:4). *Actus reus* merupakan manifestasi lahiriah dari niat atau kehendak batin pelaku, sehingga tanpa adanya perbuatan yang nyata, suatu niat tidak dapat dipidana.

Dalam hal ini, manipulasi data biometrik melalui teknologi *Artificial Intelligence* seperti *deepfake* wajah dan *voice cloning* dapat digunakan sebagai sarana untuk memenuhi unsur tipu muslihat dalam tindak pidana penipuan sebagaimana diatur dalam Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (KUHP). Selain itu, perbuatan tersebut juga dapat dikualifikasikan sebagai manipulasi informasi elektronik sebagaimana diatur dalam Pasal 35 Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang

---

melarang setiap orang melakukan manipulasi data elektronik agar seolah-olah menjadi data yang autentik.

Penggunaan Pasal 35 UU ITE dalam hal *Artificial Intelligence* sering kali menghadapi tantangan, pertanggungjawaban pidana terhadap PSE tidak serta-merta dibebankan hanya karena sistem yang dikelola digunakan untuk melakukan kejahatan. Penentuan tanggung jawab tersebut harus didasarkan pada ada atau tidaknya unsur kesalahan, baik dalam bentuk kesengajaan (*dolus*) maupun kelalaian (*culpa*) (Utoyo dkk, 2020:83). Dalam perspektif pertanggungjawaban pidana korporasi. Pertanggungjawaban pidana korporasi adalah konsep dalam hukum pidana yang menyatakan bahwa korporasi (badan hukum) dapat dimintai pertanggungjawaban atas tindak pidana yang dilakukan dalam lingkup kegiatan usahanya, baik oleh pengurus, karyawan, maupun pihak yang bertindak untuk dan atas nama korporasi tersebut (Muladi dkk, 2015). Kesalahan PSE dapat diidentifikasi melalui doktrin kelalaian korporasi (*corporate negligence*), di mana PSE dianggap "sengaja membiarkan" (*willful blindness*) risiko manipulasi biometrik terjadi demi keuntungan komersial tanpa pengawasan memadai.

Dalam praktiknya penyalahgunaan teknologi *Artificial Intelligence* seringkali dilakukan oleh pihak yang tidak bertanggung jawab tanpa sepengetahuan PSE. Dalam kondisi demikian, pertanggungjawaban pidana PSE dapat timbul apabila terdapat unsur kelalaian. Kelalaian tersebut dapat berupa tidak dipenuhinya kewajiban untuk menyelenggarakan sistem elektronik yang andal dan aman sebagaimana diatur dalam Pasal 15 ayat (1) UU ITE, serta tidak dilaksanakannya perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Selain itu, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga menegaskan bahwa PSE wajib menjamin keamanan sistem serta melindungi data pribadi pengguna dari akses yang tidak sah. Apabila PSE gagal memenuhi kewajiban tersebut sehingga mengakibatkan terjadinya manipulasi data biometrik yang merugikan pihak lain, maka PSE dapat dimintai pertanggungjawaban, baik dalam bentuk pertanggungjawaban administratif, perdata, maupun pidana.

Dalam perspektif pertanggungjawaban pidana korporasi, PSE sebagai badan hukum juga dapat dimintai pertanggungjawaban apabila tindak pidana dilakukan dalam lingkup kegiatan usahanya atau terdapat hubungan antara perbuatan pelaku dengan kepentingan korporasi. Hal ini sejalan dengan ketentuan dalam UU PDP yang mengakui adanya pertanggungjawaban pidana korporasi, sehingga sanksi tidak hanya dijatuhkan kepada individu pelaku, tetapi juga kepada badan hukum sebagai penyelenggara sistem elektronik.

Dengan demikian, pertanggungjawaban pidana PSE berbasis *Artificial Intelligence* atas manipulasi data biometrik dalam penipuan transaksi elektronik sangat bergantung pada pembuktian adanya unsur kesalahan, baik dalam bentuk kesengajaan maupun kelalaian, serta keterkaitan antara sistem yang dikelola dengan terjadinya tindak pidana. Oleh karena itu, PSE dituntut untuk menerapkan prinsip kehati-hatian (*due diligence*), meningkatkan standar keamanan sistem, serta

---

melakukan pengawasan yang ketat guna mencegah penyalahgunaan teknologi *Artificial Intelligence* dalam transaksi elektronik.

Namun, persoalan mendasar yang muncul dalam penegakan hukum saat ini adalah ketiadaan regulasi khusus (*lex specialis*) yang mengatur mengenai *Artificial Intelligence* (AI), sehingga proses pembuktian untuk meminta pertanggungjawaban Penyelenggara Sistem Elektronik (PSE) menjadi sangat sulit dilakukan. Kondisi ini menciptakan ketidakpastian dalam menentukan apakah PSE memang sengaja membiarkan sistem AI mereka digunakan untuk kejahatan demi keuntungan tertentu, ataukah mereka hanya sekadar mengembangkan fitur canggih tanpa batasan keamanan yang memadai sehingga akhirnya disalahgunakan sebagai alat kejahatan. Langkah pemerintah yang sejauh ini baru mengeluarkan Surat Edaran Menteri Kominfo Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. Padahal, secara hierarki hukum, Surat Edaran hanyalah bersifat sebagai pedoman atau arahan etis (*soft law*) yang tidak memiliki kekuatan mengikat secara umum dan tidak memuat sanksi hukum yang tegas bagi pelanggarnya. Akibatnya, tanpa adanya standar kewajiban yang memaksa dalam bentuk Undang-Undang atau Peraturan Pemerintah, PSE sering kali sulit dijerat secara hukum ketika teknologi AI yang mereka operasikan justru memfasilitasi manipulasi data biometrik dalam penipuan transaksi elektronik.

## SIMPULAN

Berdasarkan hasil analisis dan pembahasan, maka dapat ditarik dua simpulan utama: (1) Pengaturan hukum manipulasi data biometrik melalui teknologi *Artificial Intelligence* (AI) di Indonesia saat ini masih bersifat tersebar (*fragmented*) dalam beberapa regulasi utama, yaitu UU ITE (khususnya Pasal 35 mengenai manipulasi informasi elektronik), UU Pelindungan Data Pribadi (Pasal 4 dan Pasal 66 mengenai penggunaan data pribadi palsu), serta KUHP Nasional (UU No. 1/2023) terkait delik penipuan dan pemalsuan. Meskipun belum terdapat *lex specialis* yang mengatur *Artificial Intelligence*, instrumen hukum positif yang ada telah mengklasifikasikan manipulasi biometrik (seperti *deepfake* dan *voice cloning*) sebagai perbuatan melawan hukum yang dapat dipidana. (2) Pertanggungjawaban pidana Penyelenggara Sistem Elektronik (PSE) atas manipulasi data biometrik berbasis *Artificial Intelligence* dalam transaksi elektronik dapat ditarik melalui doktrin kesalahan, baik berupa kesengajaan maupun kelalaian (*corporate negligence*), sebagaimana diatur dalam UU ITE, UU PDP, dan KUHP Nasional. Namun, penegakan hukum terhadap PSE saat ini menghadapi hambatan besar akibat kekosongan regulasi khusus (*lex specialis*) yang mengatur standar teknis dan batasan tanggung jawab *Artificial Intelligence* secara tegas. Langkah pemerintah yang sejauh ini hanya menerbitkan Surat Edaran Kominfo Nomor 9 Tahun 2023 dinilai belum cukup kuat secara hierarki hukum karena hanya bersifat imbauan etis (*soft law*) tanpa sanksi yang mengikat. Oleh karena itu, diperlukan transformasi regulasi dari sekadar pedoman etika menjadi aturan hukum yang memaksa guna memberikan kepastian hukum dalam menjerat PSE yang membiarkan teknologinya menjadi sarana kejahatan digital.

**DAFTAR RUJUKAN**

- Aprianto, N. E. K. (2021). Peran teknologi informasi dan komunikasi dalam bisnis. *International Journal Administration, Business & Organization*, 2(1), 8-15.
- Ar, A. M., Wirda, W., Rusbandi, A. S., Zuhendra, M., Bahri, S., & Fajri, D. (2024). Peran Niat (Mens rea) dalam Pertanggungjawaban Pidana di Indonesia. *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, 1(3), 240-252.
- CDM, I. G. A. D. L., Yuliantini, N. P. R., & Mangku, D. G. S. (2020). Penjatuhan Sanksi Terhadap Pelaku Tindak Pidana Pembunuhan (Studi Kasus Di Pengadilan Negeri Singaraja Dalam Perkara NO. 124/PID. B/2019/PN. SGR). *Jurnal Komunitas Yustisia*, 3(1), 48-58.
- Haris, M. T. A. R., & Tantimin, T. (2022). Analisis pertanggungjawaban hukum pidana terhadap pemanfaatan artificial intelligence di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, 8(1), 307-316.
- Hartono, M. S., & Yuliantini, N. P. R. (2020). Penggunaan bukti elektronik dalam peradilan pidana. *Jurnal Komunikasi Hukum (JKH)*, 6(1), 281-302.
- Heidari, A., Jafari Navimipour, N., Dag, H., & Unal, M. (2024). Deepfake detection using deep learning methods: A systematic and comprehensive review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 14(2), e1520.
- Junita Melo, I., & Arthur Novy Tuwaidan, M. (2025). Metode Penelitian Dan Penulisan Hukum, Eureka Media Aksara, Kecamatan Bojongsari Kabupaten Purbalingga, Jawa Barat
- Ks, Y. S., Ablisar, M., Mulyadi, M., & Leviza, J. (2022). Analisis Yuridis Terhadap Tindak Pidana Manipulasi Informasi Pengguna E-Commerce Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik: Studi Putusan No. 542/Pid. Sus/2019/PN. Mlg. *Locus: Jurnal Konsep Ilmu Hukum*, 2(2), 53-67.
- Kusuma, P. R. A., & Sanjaya, D. B. (2024). Analisis Pasal 100 Undang-Undang Nomor 1 Tahun 2023 Tentang Hukuman Mati Bersyarat Berdasarkan Asas Keadilan Dan Asas Kepastian Hukum. *Jurnal Ilmu Hukum Sui Generis*, 4(3).
- Mangku, D. G. S., Yuliantini, N. P. R., & Lasmawan, I. W. (2022). Legal Protection for People with Disabilities in Indonesia in the Perspective of Justice Theory. *Unnes Law Journal*, 8(2), 245-262.
- Parwati, N. P. E. (2024). Tantangan Sistem Pemidanaan Terhadap Anak Sebagai Pelaku Tindak Pidana Dalam Sistem Peradilan Pidana Anak Di Indonesia. *Jurnal Locus Delicti*, 5(2), 98-114.
- Romandona, R., & Yasin, B. (2024). Analisis Hukum Asas Mens Rea Dan Actus Reus Dalam Kasus Pembunuhan Brigadir Nofriansyah Yosua Hutabarat (Studi Kasus Dalam Putusan Pn Jakarta Selatan No. 796/Pid. B/2022/Pn Jkt. Sel). *JUSTITIABLE-Jurnal Hukum*, 6(2), 1-12.
- Sukmaningsih, N. K. I. A. (2025, January). Urgensi pengaturan hak cipta di era kecerdasan buatan: Tantangan dan solusi hukum di Indonesia. In *Prosiding Seminar Nasional Hukum, Bisnis, Sains dan Teknologi* (Vol. 5, No. 1, pp. 16-22).
- Syaifudin, A., Yahya, M., Putri, N., Angelica, R., Akbar, S., Khalil, S., & Ardina, T. (2025). E-commerce dalam transformasi digital: Menciptakan peluang baru

- berkelanjutan untuk bisnis modern. *Jurnal Pembelajaran Pemberdayaan Masyarakat (JP2M)*, 6(4), 1074-1084.
- Trisiana, A., & Wartoyo, W. (2025). Peningkatan Pemberdayaan Masyarakat Di Desa Mlese Melalui Implementasi Aplikasi Smart Village Sebagai Pendukung Literasi Digital Desa Pelopor Pancasila. *Jurnal Global Citizen: Jurnal Ilmiah Kajian Pendidikan Kewarganegaraan*, 14(2), 46-58.
- Utoyo, M., Afriani, K., Rusmini, R., & Husnaini, H. (2020). Sengaja Dan Tidak Sengaja Dalam Hukum Pidana Indonesia. *Lex Librum*, 7(1), 75-85.
- Windari, RA, & Dewi, YK (2024). Evaluasi kebijakan pengungkapan tanggung jawab sosial perusahaan yang wajib dan pencapaian tujuan pembangunan berkelanjutan di Indonesia. *Yustisia*, 13 (1), 1-26.
- Yudiawan, I. D. G. H., Hartono, M. S., & Yasmiati, N. L. W. (2023). Kewenangan Komisi Penyiaran Indonesia Terhadap Pengawasan Jasa Penyiaran Berbasis Internet. *Ganesha Law Review*, 5(1), 78-93.
- Yuliantini, N. P. R. (2015). Kedudukan korban kejahatan dalam sistem peradilan pidana di Indonesia berdasarkan Kitab Undang-Undang Hukum Acara Pidana (KUHP). *Jurnal Komunikasi Hukum (JKH)*, 1(1).
- Yuliantini, N. P. R., Pramita, K. D., & Yasmiati, N. L. W. (2022). Analysis Of Workload, Rest Rights, And The Rights To Enjoy Entertainment In Gender Differences. *Jurnal Komunikasi Hukum (JKH)*, 8(1), 469-480.
- Muladi, D. R., Priyatno, D. D., & MH, S. (2015). *Pertanggungjawaban Pidana Korporasi: Edisi Ketiga*. Kencana.
- Rojabi, M. A. (2025). *Pengantar Artificial Intelligence (AI)*. Afdan Rojabi Publisher.
- Kitab Undang-Undang Hukum Pidana
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
- Undang-Undang Nomor 19 Tahun 2019 tentang Informasi dan Transaksi Elektronik
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik
- Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik
- Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial
- Ermeitha, Vionna (2025) Penerapan Teknologi Biometrik Dalam Sistem Modern Dan Dampaknya Terhadap Keamanan Transaksi Bank Syariah. Tesis Sarjana (S1), Uin Fatmawati Sukarno Bengkulu.